КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.33.1239
УДК 004.89

Yuriy Myshkovskyi
Postgraduate student, Department of Information Systems and Networks
National University "Lviv Polytechnic", Lviv, Ukraine
ORCID: 0009-0004-0051-026X
yurii.i.myshkovskyi@lpnu.ua

Mariia Nazarkevych
Doctor of Technical Sciences, Professor,
Professor, Department of Information Systems and Networks
National University "Lviv Polytechnic", Lviv, Ukraine
Ivan Franko National University of Lviv, Lviv, Ukraine
ORCID: 0000-0002-6528-9867
Mariia.a.nazarkevych@lpnu.ua

METHOD OF PROTECTING FINGERPRINTS IN AN INTELLIGENT DECISION-MAKING SYSTEM BASED ON CONVULSIVE NEURAL NETWORKS

Abstract. The article investigates the problem of detecting fingerprint "liveness" as an important element of ensuring cybersecurity of modern biometric authentication systems. It is substantiated that the widespread use of biometrics in financial services, corporate networks, mobile applications and e-government systems is accompanied by an increase in the risks of spoofing attacks, during which attackers use artificial or modified fingerprints to bypass identification mechanisms. An approach to solving this problem is proposed based on convolutional neural networks, capable of automatically identifying discriminative features of images, in particular textural features, papillary line structure violations and artifacts characteristic of counterfeit samples. Experimental studies were performed using the SocoFing dataset with a constant model configuration and training parameters. The results obtained demonstrate the high efficiency of the approach: the classification accuracy is 98.964%, the false acceptance rate (FAR) is 0.215%, and the false rejection rate (FRR) is 7.251%. A low FAR value indicates the model's ability to minimize the risk of unauthorized access, which is critically important for systems with increased security requirements. At the same time, an increased level of FRR indicates the need for further optimization to ensure a balance between security and usability. It is concluded that models based on deep learning can be effectively used as an additional layer of protection in biometric systems, especially in the context of multi-factor authentication and the concept of zero trust. Directions for further research are outlined, in particular, the use of more diverse data sets, increasing resistance to new types of attacks, and integration with other cyber defense mechanisms.

Keywords: cybersecurity, biometric authentication, fingerprint liveness detection, convolutional neural networks, presentation attack detection, spoofing attacks, access control, FAR, FRR.

INTRODUCTION

Biometric authentication is increasingly used as a cybersecurity mechanism for protecting digital services, physical infrastructure, financial transactions, and enterprise resources. Unlike passwords or tokens, biometric characteristics are directly associated with the user and therefore reduce risks connected with forgotten credentials, weak passwords, password reuse, and credential sharing. Fingerprints remain one of the most widely adopted biometric modalities because scanners are compact, inexpensive, and already integrated into laptops, smartphones, and access-control terminals [1, 2].

However, biometric authentication does not eliminate cybersecurity risk. It changes the attack surface. Instead of stealing a password, an attacker may attempt to deceive the biometric sensor with a fake, modified, or synthetic fingerprint. Such attacks are known as presentation attacks or spoofing attacks. In a cybersecurity context, successful fingerprint spoofing can lead to unauthorized login, privilege escalation, fraudulent transactions, or bypassing multi-factor authentication in systems that rely heavily on biometric factors [3, 4].

Fingerprint liveness detection is therefore a necessary defense mechanism. Its task is to determine whether the biometric sample originates from a live human finger rather than an artifact. In practice, liveness

detection becomes part of the identity assurance pipeline: sensor capture, feature extraction, liveness verification, identity matching, decision making, logging, and response. Recent research on biometric anti-spoofing and liveness detection confirms that presentation attack detection must be treated as a continuously evolving security problem because attack materials and fabrication techniques improve over time [5, 6].

Deep learning, and specifically Convolutional Neural Networks (CNNs), is well suited for this task because fingerprint images contain local ridge patterns, pores, distortions, texture irregularities, and artifacts that can be learned from image data. CNNs are widely used in visual recognition tasks and can automatically extract hierarchical features from raw images [7]. In this article, the original fingerprint liveness detection study is rewritten with an explicit cybersecurity orientation while preserving the same experimental dataset, architecture, training settings, evaluation metrics, results, figures, and reference list.

Problem statement. Fingerprint systems may be attacked using artificial fingerprints created from silicone, gelatin, printed patterns, or digitally altered fingerprint images. Traditional fingerprint recognition systems mainly verify identity similarity and may not reliably distinguish a live finger from an artifact. Therefore, a robust liveness detection subsystem is needed to detect spoofing attempts before the identity-matching decision is trusted.

The research problem addressed in this article is the development and evaluation of a CNN-based liveness detection model for distinguishing genuine and spoofed fingerprints under a cybersecurity threat model. The model must be evaluated not only by overall accuracy but also by FAR and FRR, because these metrics directly correspond to security failure and usability failure.

1.1 Cybersecurity relevance of fingerprint liveness detection. In cybersecurity practice, biometric liveness detection supports several defensive objectives:

- Prevention of unauthorized access. A liveness model reduces the probability that a fake fingerprint is accepted as a legitimate biometric factor.
- Protection of high-value accounts. In banking, healthcare, government portals, and corporate environments, biometric spoofing may enable fraud or exposure of sensitive data [2, 4].
- Strengthening multi-factor authentication. If a biometric factor is compromised through spoofing, the overall authentication chain weakens. Liveness detection increases assurance that the biometric factor is valid.
- Support for zero-trust access control. Modern access decisions require continuous verification and risk scoring; liveness detection provides an additional signal for identity confidence.
- Reduction of insider and physical access risks. Biometric terminals used in offices, laboratories, and critical infrastructure can be targeted with fake biometric artifacts.

Thus, the main cybersecurity question is not only whether the CNN can classify images accurately, but whether it reduces security-critical errors. In this study, the most important security metric is the False Acceptance Rate (FAR), because it measures how often a spoofed fingerprint is incorrectly accepted as genuine. At the same time, the False Rejection Rate (FRR) remains important because excessive rejection of genuine users can reduce system usability and cause operational problems [8, 9].

Related work and cybersecurity context. Biometric technologies are widely discussed in the context of migration control, banking, authentication, and security governance [1, 2, 3]. In cybersecurity applications, biometric systems are attractive because they bind access decisions to human physiological or behavioral traits. Nevertheless, biometric authentication is probabilistic and cannot be treated as an absolute guarantee of identity [15, 16].

Recent works emphasize both the practical value and the security risks of biometric systems. Cancellable biometric approaches and transformed biometric templates are proposed for cybersecurity applications where biometric data protection is required [4]. Liveness detection methods are studied across multiple biometric modalities, including fingerprint and sclera biometrics [5]. The LivDet competition series demonstrates that fingerprint liveness detection has progressed significantly but remains a challenging problem because sensors, datasets, and attack materials vary over time [6, 8].

CNN-based methods are relevant because they can learn discriminative spatial features directly from images. A CNN can detect local fingerprint texture differences, abnormal ridge continuity, artifacts caused by spoof materials, and distortions introduced by modification or fabrication. General studies of CNNs confirm their effectiveness in image classification and feature extraction tasks [7]. For biometric image analysis, related research also includes latent biometric image identification and image processing methods for biometric security systems [12, 14].

From the cybersecurity perspective, this article treats fingerprint liveness detection as an anti-spoofing control. The main risk is not a random classification error but a security breach caused by accepting an attack sample as genuine. Therefore, FAR is interpreted as a direct attack-success indicator, while FRR is interpreted as a legitimate-user denial indicator.

The purpose of the article.

1. To design and train a CNN model for fingerprint liveness detection using the SocoFing dataset [10]. 2. To preserve the experimental setup of the original study while interpreting the results as cybersecurity controls.3. To evaluate the model using accuracy, FAR, FRR, and confusion matrix analysis [9, 12]. 4.To identify how the model can be used in practical biometric security systems [13, 14]. 5.To outline future improvements for more resilient biometric anti-spoofing systems.

METHODOLOGY

Dataset SocoFing. The research uses the SocoFing dataset, which contains fingerprint images suitable for experiments with real and altered fingerprints. The dataset was introduced as the Sokoto Coventry Fingerprint Dataset and is used for fingerprint recognition and biometric research [10]. In this study, it supports a binary liveness detection task: distinguishing genuine fingerprints from spoofed or modified fingerprints.

The dataset is appropriate for cybersecurity-oriented analysis because it includes different fingerprint conditions and modified samples that simulate adversarial or non-genuine biometric presentations. Before training, images were resized, normalized, and augmented to improve generalization. The use of preprocessing is important for practical deployment because real biometric systems receive data with variable quality, orientation, pressure, and sensor noise.

Figure 1: SocoFing dataset examples. The first row presents real fingerprints, the second row presents slightly modified fingerprints, and the third row presents greatly modified fingerprints

Threat model

The cybersecurity threat model assumes that an attacker attempts to pass fingerprint authentication without being the legitimate user. The attack may involve a fabricated fingerprint, an altered fingerprint image, or an artifact presented to the sensor. The defender deploys a CNN-based liveness detection module before final authentication approval.

The model output is interpreted as follows:

- Genuine/live: the biometric sample is likely from a legitimate living finger.
- Spoof/non-live: the biometric sample is likely an artificial or modified presentation.

In operational systems, the liveness result can be integrated into access-control policies. For example, a suspicious liveness score can trigger denial, step-up authentication, manual review, or risk-based logging.

CNN architecture.

The primary model is a Convolutional Neural Network. The architecture preserves the original experimental design and consists of an input layer, two convolutional blocks, flattening, a dense layer, and a softmax output layer.

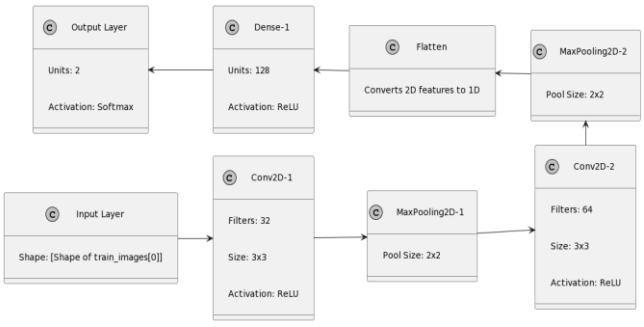

Figure 2: Architecture of the CNN model for cybersecurity-oriented fingerprint liveness detection.

The architecture includes:

1. Input layer. Accepts fingerprint image pixel values.
2. First Conv2D layer. Uses 32 filters with a 3x3 kernel and ReLU activation.
3. First MaxPooling2D layer. Uses a 2x2 pool size to reduce spatial dimensions.
4. Second Conv2D layer. Uses 64 filters with a 3x3 kernel and ReLU activation.
5. Second MaxPooling2D layer. Uses a 2x2 pool size.
6. Flatten layer. Converts 2D feature maps into a 1D vector.
7. Dense layer. Uses 128 neurons with ReLU activation.
8. Output layer. Uses 2 neurons and softmax activation for the genuine/spoof classification.

This architecture is lightweight enough for security systems where inference speed is important, while still providing hierarchical feature extraction from fingerprint images.

Model compilation and training. The model was trained using the Adam optimizer with a learning rate of 0.001. Adam is widely used for deep neural network optimization because it adapts learning rates during training and combines advantages of momentum-based and adaptive gradient methods [11]. The loss function was categorical cross-entropy for the two-class classification problem.

The preserved training settings are:

- Training-validation split: 80% / 20%.
- Batch size: 2764.
- Number of epochs: 10.
- Optimizer: Adam.
- Learning rate: 0.001.
- Task: binary classification of genuine and spoofed fingerprints.

Evaluation metrics. The model was evaluated using metrics that are meaningful for cybersecurity decision making:

- Accuracy: proportion of all correctly classified samples.
- False Acceptance Rate (FAR): proportion of spoofed fingerprints incorrectly accepted as genuine.
- False Rejection Rate (FRR): proportion of genuine fingerprints incorrectly rejected as spoofed.
- Confusion matrix: detailed count of true positives, false positives, true negatives, and false negatives.

For cybersecurity, FAR is especially important because a false acceptance corresponds to a potential unauthorized access event. FRR is also important because too many false rejections can reduce availability and usability, leading users or administrators to weaken security controls.

RESEARCH RESULTS

Training and validation dynamics. The same experimental data from the original study are reused. Table 1 presents the loss and accuracy values for the 10 training epochs.

Table 1

Model training and validation metrics for each epoch

Epoch	Loss	Accuracy	Validation Loss	Validation Accuracy
1	0.1742	0.9260	0.1342	0.9378
2	0.0751	0.9694	0.0650	0.9761
3	0.0482	0.9813	0.0634	0.9755
4	0.0348	0.9866	0.0375	0.9860
5	0.0260	0.9905	0.0267	0.9910
6	0.0189	0.9931	0.0350	0.9869
7	0.0162	0.9940	0.0246	0.9919
8	0.0131	0.9952	0.0252	0.9935
9	0.0116	0.9958	0.0321	0.9923
10	0.0116	0.9959	0.0368	0.9896

The training accuracy increased from 0.9260 to 0.9959, while validation accuracy remained high and reached 0.9896 at epoch 10. From a cybersecurity perspective, this indicates that the model learned stable image features rather than only memorizing the training samples. The validation curve also suggests that the model can generalize to unseen fingerprint images, which is essential for real-world authentication systems.

ISSN 2663 – 4023

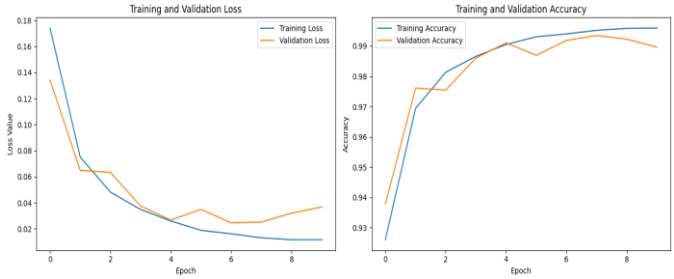

Figure 3: Training and validation loss and accuracy curves

Final performance metrics. The final preserved test results are:

- Accuracy: 98.964%.
- False Acceptance Rate (FAR): 0.215%.
- False Rejection Rate (FRR): 7.251%.

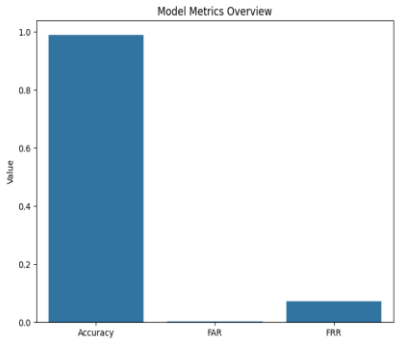

Figure 4: Performance metrics of the liveness detection model: accuracy, FAR, and FRR

The low FAR is the most significant cybersecurity result. A FAR of 0.215% means that the model rarely accepts spoofed fingerprints as genuine. In a high-security biometric system, this property is critical because false acceptance can lead directly to unauthorized access. However, the FRR of 7.251% indicates that some legitimate users may be rejected. In practical systems, this can be mitigated by step-up authentication, repeated capture, user feedback, or fallback authentication.

Confusion matrix analysis. The preserved confusion matrix values are:

- True Positives (TP): 2392.
- False Positives (FP): 42.
- True Negatives (TN): 19487.
- False Negatives (FN): 187.

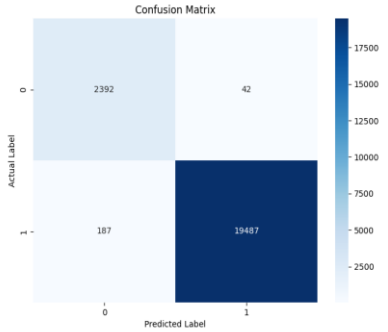

Figure 5: Confusion matrix for CNN-based fingerprint liveness detection

The confusion matrix shows that the model correctly classified a large number of genuine and spoofed samples. The 42 false positives represent the main cybersecurity concern because they correspond to spoofed fingerprints incorrectly treated as genuine. The 187 false negatives represent legitimate-user rejection. In cybersecurity deployment, these two error types should be handled differently: false positives require stricter anti-spoofing controls, while false negatives require usability-oriented recovery mechanisms.

Cybersecurity analysis of the results.

Interpretation of FAR as attack-success probability. In traditional machine-learning analysis, FAR is one of several performance metrics. In cybersecurity, FAR has a more direct operational meaning: it estimates how frequently spoofing attempts may be accepted by the biometric liveness subsystem. The obtained FAR of 0.215% is promising because it indicates strong resistance against spoof samples in the evaluated dataset.

Nevertheless, even a low FAR must be interpreted according to system scale. In a large enterprise or banking environment, thousands or millions of authentication attempts may occur over time. A small percentage of false acceptance may still translate into security incidents. Therefore, CNN-based liveness detection should not be treated as a standalone protection layer; it should be integrated with risk-based authentication, device trust, anomaly detection, secure logging, and anti-fraud monitoring.

Interpretation of FRR as availability and usability risk

The FRR of 7.251% means that some genuine users may be rejected. In cybersecurity, availability is one of the core security properties alongside confidentiality and integrity. A system that frequently rejects legitimate users may cause operational disruption, helpdesk load, and user frustration. In practice, high FRR can also create indirect security risks: users may pressure administrators to disable biometric checks or choose weaker fallback mechanisms.

For this reason, biometric security systems should implement controlled fallback paths. Examples include re-capture, additional fingerprint attempt, multi-factor verification, hardware token confirmation, or administrator-reviewed recovery for high-value systems.

Deployment implications. The results support the use of CNN-based liveness detection as part of biometric cybersecurity systems. Possible deployment scenarios include:

- Mobile banking and payment confirmation. Liveness detection can reduce fraud caused by fake fingerprints [2].
- Enterprise workstation login. A CNN-based module can strengthen biometric login where fingerprint scanners are used.
- Physical access control. Liveness checks can protect restricted areas and critical infrastructure.
- E-government and digital identity. Biometric liveness detection can improve trust in remote identity verification.
- Zero-trust identity systems. The liveness score can become an additional risk signal in adaptive access decisions.

However, deployment requires protection of the entire biometric pipeline. The CNN model must be combined with secure sensor communication, template protection, secure storage, audit logging, and privacy-preserving processing. Biometric templates and liveness decisions are sensitive security assets and must be protected against leakage, tampering, replay, and model extraction.

Comparison with broader biometric security research. The obtained results are consistent with the broader direction of biometric security research, where image processing, biometric template protection, and recognition methods are used to improve security and reliability [12, 13, 14]. At the same time, biometric systems remain probabilistic and must be evaluated within the full security context [15, 16]. Studies of cloud data warehouses, medical data processing, and protection-system modeling also show that secure information systems require integrated approaches to data protection, decision making, and system design [17, 18, 19].

Limitations and challenges. Several limitations remain important for cybersecurity deployment:

- Dataset dependence. The model was evaluated on SocoFing, and performance may change with other sensors, populations, spoof materials, and environmental conditions [10].
- Presentation attack diversity. Real attackers may use spoofing materials or fabrication methods not represented in the dataset [6].
- Adversarial adaptation. Attackers may adapt to known detection methods, requiring continuous model updates.
- Operational threshold selection. Security systems may need different thresholds depending on the acceptable balance between FAR and FRR.
- Privacy and compliance. Biometric data must be stored and processed according to legal, ethical, and cybersecurity requirements.
- Model security. The CNN itself can become a target of adversarial attacks, model inversion, or tampering if deployed insecurely.

Recommendations for cybersecurity implementation. Based on the preserved experimental results, the following recommendations are proposed:

- Use CNN liveness detection as an additional security layer, not as a standalone authentication system.

- Prioritize FAR reduction for high-security applications. In systems where unauthorized access is unacceptable, reducing false acceptance is more important than maximizing convenience.
- Use adaptive thresholds. High-risk login events may require stricter liveness thresholds than routine low-risk access.
- Add fallback authentication for genuine users. Because the FRR is 7.251%, systems should support secure recovery paths.
- Continuously retrain and validate the model. New spoofing materials and sensor types require updated training data.
- Secure the biometric pipeline. Sensor communication, template storage, model inference, logs, and access decisions must be protected.
- Evaluate with additional metrics. In future work, Matthews Correlation Coefficient (MCC), ROC analysis, and attack-presentation classification error rates can provide a more complete evaluation [9].

CONCLUSIONS AND PROSPECTS FOR FURTHER RESEARCH

This article presented a cybersecurity-oriented rewrite of a CNN-based fingerprint liveness detection study while preserving the original experimental data and reference list. The CNN model achieved 98.964% accuracy, a FAR of 0.215%, and an FRR of 7.251% on the SocoFing dataset. The low FAR is the key cybersecurity result because it indicates that the model rarely accepts spoofed fingerprints as genuine. This makes CNN-based fingerprint liveness detection a promising anti-spoofing mechanism for biometric authentication systems.

At the same time, the FRR indicates that the model should be improved before deployment in systems where user availability and authentication reliability are critical. Future work should focus on larger and more diverse datasets, transfer learning, hybrid architectures, advanced augmentation, adversarial robustness testing, and continuous model monitoring. In practical cybersecurity systems, CNN-based liveness detection should be combined with multi-factor authentication, secure biometric template management, audit logging, and adaptive risk-based access control.

Acknowledgments

The research was conducted with the grant support of the National Research Foundation of Ukraine "Methods of analysis and optimization of multimodal data for deep learning models in the military sphere", project registration №. 2025.07/0017 dated 12/24/2025.

REFERENCES

1. Iwuoha, V. C., & Doevenspeck, M. (2023). Dilemmas of “biometric nationality”: Migration control, biometric ID technology, and political mobilisation of migrants in West Africa. *Territory, Politics, Governance*, 1-26.
2. Marani, M., Soltani, M., Bahadori, M., Soleimani, M., & Moshayedi, A. (2023). The role of biometrics in banking: A review. *EAI Endorsed Transactions on AI and Robotics, 2*(1).
3. El-Afifi, M. I., & El Kelany, M. M. (2023). Trends in biometric authentication: A review. *Nile Journal of Communication and Computer Science*.
4. Helmy, M., El-Rabaie, E. S. M., El-Dokany, I., & Abd El-Samie, F. E. (2023). A novel cancellable biometric recognition system based on Rubik’s cube technique for cybersecurity applications. *Optik, 285*, 170475.
5. Das, S., De Ghosh, I., & Chattopadhyay, A. (2023). A liveness detection system for sclera biometric applications. *International Journal of Biometrics, 15*(6), 645-664.
6. Micheletto, M., Orrù, G., Casula, R., Yambay, D., Marcialis, G. L., & Schuckers, S. (2023). Review of the Fingerprint Liveness Detection (LivDet) competition series: From 2009 to 2021. In *Handbook of Biometric Anti-Spoofing: Presentation Attack Detection and Vulnerability Assessment* (pp. 57-76).
7. Krichen, M. (2023). Convolutional neural networks: A survey. *Computers, 12*(8), 151.
8. Micheletto, M., Orrù, G., Casula, R., Yambay, D., Marcialis, G. L., & Schuckers, S. (2023). Review of the Fingerprint Liveness Detection (LivDet) competition series: From 2009 to 2021. In *Handbook of Biometric Anti-Spoofing: Presentation Attack Detection and Vulnerability Assessment* (pp. 57-76).
9. Chicco, D., & Jurman, G. (2023). The Matthews correlation coefficient (MCC) should replace the ROC AUC as the standard metric for assessing binary classification. *BioData Mining, 16*(1), 1-23.
10. Shehu, Y. I., Ruiz-Garcia, A., Palade, V., & James, A. (2018). *Sokoto Coventry fingerprint dataset*. arXiv. https://arxiv.org/abs/1807.10609

11. Sun, H., Shen, L., Zhong, Q., Ding, L., Chen, S., Sun, J., et al. (2023). *AdaSAM: Boosting sharpness-aware minimization with adaptive learning rate and momentum for training deep neural networks*. arXiv. https://arxiv.org/abs/2303.00565
12. Logoyda, M., Nazarkevych, M., Voznyi, Y., Dmytruk, S., & Smotr, O. (2019). Identification of biometric images using latent elements. In *CEUR Workshop Proceedings*.
13. Dronyuk, I., Nazarkevych, M., & Poplavska, Z. (2017). Gabor filters generalization based on ateb-functions for information security. In *International Conference on Man-Machine Interactions* (pp. 195-206). Springer.
14. Nazarkevych, M., Dmytruk, S., Hrytsyk, V., Vozna, O., Kuza, A., Shevchuk, O., et al. (2021). Evaluation of the effectiveness of different image skeletonization methods in biometric security systems. *International Journal of Sensors, Wireless Communications and Control, 11*(5), 542-552. https://doi.org/10.2174/2210327910666201210151809
15. Sheketa, V., Romanyshyn, Y., Vovk, R., Pikh, V., & Pasyeka, M. (2019). Formal methods for solving technological problems in the infocommunications routines of intelligent decision-making for drilling control. In *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)* (pp. 29-34). IEEE.
16. Sheketa, V., Zorin, V., Chupakhina, S., Kyrsta, N., Pasyeka, M., & Pasieka, N. (2020). Empirical method of evaluating the numerical values of metrics in the process of medical software quality determination. In *2020 International Conference on Decision Aid Sciences and Application (DASA)* (pp. 22-26). IEEE.
17. Shakhovska, N., Boyko, N., & Pukach, P. (2018). The information model of cloud data warehouses. In *Conference on Computer Science and Information Technologies* (pp. 182-191).
18. Nazarkevych, M., Vysotska, V., Yurynets, R., & Nakonechny, N. (2025). Methods of implementing disinformation detection in social networks based on artificial intelligence. *Cybersecurity: Education, Science, Technique, 2*(30), 209-223. https://doi.org/10.28925/2663-4023.2025.30.965
19. Myshkovskyi, Y., Nazarkevych, M., & Klyujnyk, I. (2025). Research on the performance of a neural network for recognizing combat vehicles. In *2025 IEEE 13th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)* (pp. 1-4). IEEE.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023

Мишковський Юрій Ігорович
аспірант кафедри інформаційних систем і мереж
Національний університет «Львівська політехніка», Львів, Україна
ORCID: 0009-0004-0051-026X
yurii.i.myshkovskyi@lpnu.ua

Назаркевич Марія Андріївна
доктор технічних наук, професор,
професор кафедри інформаційних систем і мереж
Національний університет «Львівська політехніка», Львів, Україна
Львівський національний університет імені Івана Франка, Львів, Україна
ORCID: 0000-0002-6528-9867
Mariia.a.nazarkevych@lpnu.ua

МЕТОД ЗАХИСТУ ВІДБИТКІВ ПАЛЬЦІВ В ІНТЕЛЕКТУАЛЬНІЙ СИСТЕМІ ПРИЙНЯТТЯ РІШЕНЬ НА ОСНОВІ ЗГОРТКОВИХ НЕЙРОННИХ МЕРЕЖ

Анотація. У статті досліджується проблема виявлення «живості» відбитків пальців як важливого елемента забезпечення кібербезпеки сучасних систем біометричної автентифікації. Обґрунтовано, що широке використання біометрії у фінансових послугах, корпоративних мережах, мобільних додатках та системах електронного урядування супроводжується зростанням ризиків спуфінг-атак, під час яких зловмисники використовують штучні або модифіковані відбитки пальців для обходу механізмів ідентифікації. Запропоновано підхід до вирішення цієї проблеми на основі згорткових нейронних мереж, здатних автоматично ідентифікувати розпізнавальні ознаки зображень, зокрема текстурні особливості, порушення структури папілярних ліній та артефакти, характерні для підроблених зразків. Експериментальні дослідження проводилися з використанням набору даних SocoFing з постійною конфігурацією моделі та параметрами навчання. Отримані результати демонструють високу ефективність підходу: точність класифікації становить 98,964%, коефіцієнт помилкових прийняття (FAR) – 0,215%, а коефіцієнт помилкових відхилень (FRR) – 7,251%. Низьке значення FAR вказує на здатність моделі мінімізувати ризик несанкціонованого доступу, що критично важливо для систем з підвищеними вимогами безпеки. Водночас, підвищений рівень FRR вказує на необхідність подальшої оптимізації для забезпечення балансу між безпекою та зручністю використання. Зроблено висновок, що моделі на основі глибокого навчання можуть бути ефективно використані як додатковий рівень захисту в біометричних системах, особливо в контексті багатофакторної автентифікації та концепції нульової довіри. Окреслено напрямки подальших досліджень, зокрема, використання більш різноманітних наборів даних, підвищення стійкості до нових типів атак та інтеграція з іншими механізмами кіберзахисту.

Ключові слова: кібербезпека, біометрична автентифікація, виявлення «живучості» відбитків пальців, згорткові нейронні мережі, виявлення атаки презентації, атаки підміни, контроль доступу, FAR, FRR.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Iwuoha, V. C., & Doevenspeck, M. (2023). Dilemmas of “biometric nationality”: Migration control, biometric ID technology, and political mobilisation of migrants in West Africa. *Territory, Politics, Governance*, 1-26.
2. Marani, M., Soltani, M., Bahadori, M., Soleimani, M., & Moshayedi, A. (2023). The role of biometrics in banking: A review. *EAI Endorsed Transactions on AI and Robotics, 2*(1).
3. El-Afifi, M. I., & El Kelany, M. M. (2023). Trends in biometric authentication: A review. *Nile Journal of Communication and Computer Science*.
4. Helmy, M., El-Rabaie, E. S. M., El-Dokany, I., & Abd El-Samie, F. E. (2023). A novel cancellable biometric recognition system based on Rubik’s cube technique for cybersecurity applications. *Optik, 285*, 170475.
5. Das, S., De Ghosh, I., & Chattopadhyay, A. (2023). A liveness detection system for sclera biometric applications. *International Journal of Biometrics, 15*(6), 645-664.

6. Micheletto, M., Orrù, G., Casula, R., Yambay, D., Marcialis, G. L., & Schuckers, S. (2023). Review of the Fingerprint Liveness Detection (LivDet) competition series: From 2009 to 2021. In *Handbook of Biometric Anti-Spoofing: Presentation Attack Detection and Vulnerability Assessment* (pp. 57-76).
7. Krichen, M. (2023). Convolutional neural networks: A survey. *Computers*, *12*(8), 151.
8. Micheletto, M., Orrù, G., Casula, R., Yambay, D., Marcialis, G. L., & Schuckers, S. (2023). Review of the Fingerprint Liveness Detection (LivDet) competition series: From 2009 to 2021. In *Handbook of Biometric Anti-Spoofing: Presentation Attack Detection and Vulnerability Assessment* (pp. 57-76).
9. Chicco, D., & Jurman, G. (2023). The Matthews correlation coefficient (MCC) should replace the ROC AUC as the standard metric for assessing binary classification. *BioData Mining*, *16*(1), 1-23.
10. Shehu, Y. I., Ruiz-Garcia, A., Palade, V., & James, A. (2018). *Sokoto Coventry fingerprint dataset*. arXiv. https://arxiv.org/abs/1807.10609
11. Sun, H., Shen, L., Zhong, Q., Ding, L., Chen, S., Sun, J., et al. (2023). *AdaSAM: Boosting sharpness-aware minimization with adaptive learning rate and momentum for training deep neural networks*. arXiv. https://arxiv.org/abs/2303.00565
12. Logoyda, M., Nazarkevych, M., Voznyi, Y., Dmytruk, S., & Smotr, O. (2019). Identification of biometric images using latent elements. In *CEUR Workshop Proceedings*.
13. Dronyuk, I., Nazarkevych, M., & Poplavska, Z. (2017). Gabor filters generalization based on ateb-functions for information security. In *International Conference on Man-Machine Interactions* (pp. 195-206). Springer.
14. Nazarkevych, M., Dmytruk, S., Hrytsyk, V., Vozna, O., Kuza, A., Shevchuk, O., et al. (2021). Evaluation of the effectiveness of different image skeletonization methods in biometric security systems. *International Journal of Sensors, Wireless Communications and Control*, *11*(5), 542-552. https://doi.org/10.2174/2210327910666201210151809
15. Sheketa, V., Romanyshyn, Y., Vovk, R., Pikh, V., & Pasyeka, M. (2019). Formal methods for solving technological problems in the infocommunications routines of intelligent decision-making for drilling control. In *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)* (pp. 29-34). IEEE.
16. Sheketa, V., Zorin, V., Chupakhina, S., Kyrsta, N., Pasyeka, M., & Pasieka, N. (2020). Empirical method of evaluating the numerical values of metrics in the process of medical software quality determination. In *2020 International Conference on Decision Aid Sciences and Application (DASA)* (pp. 22-26). IEEE.
17. Shakhovska, N., Boyko, N., & Pukach, P. (2018). The information model of cloud data warehouses. In *Conference on Computer Science and Information Technologies* (pp. 182-191).
18. Nazarkevych, M., Vysotska, V., Yurynets, R., & Nakonechny, N. (2025). Methods of implementing disinformation detection in social networks based on artificial intelligence. *Cybersecurity: Education, Science, Technique*, *2*(30), 209-223. https://doi.org/10.28925/2663-4023.2025.30.965
19. Myshkovskyi, Y., Nazarkevych, M., & Klyujnyk, I. (2025). Research on the performance of a neural network for recognizing combat vehicles. In *2025 IEEE 13th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)* (pp. 1-4). IEEE.

Отримано редакцією журналу / Received: 24.02.26
Прорецензовано / Revised: 10.03.26
Схвалено до друку / Accepted: 25.06.26